Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, and Lenka Mareková, *Royal Holloway, University of London*

https://www.usenix.org/conference/usenixsecurity21/presentation/albrecht

This paper is included in the Proceedings of the 30th USENIX Security Symposium.

August 11–13, 2021

978-1-939133-24-3

Open access to the Proceedings of the 30th USENIX Security Symposium is sponsored by USENIX.

Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht
Royal Holloway, University of London
martin.albrecht@rhul.ac.uk

Jorge Blasco
Royal Holloway, University of London
jorge.blascoalis@rhul.ac.uk

Rikke Bjerg Jensen
Royal Holloway, University of London
rikke.jensen@rhul.ac.uk

Lenka Mareková
Royal Holloway, University of London
lenka.marekova.2018@rhul.ac.uk

Abstract

The Anti-Extradition Law Amendment Bill protests in Hong Kong present a rich context for exploring information security practices among protesters due to their large-scale urban setting and highly digitalised nature. We conducted in-depth, semi-structured interviews with 11 participants of these protests. Research findings reveal how protesters favoured Telegram and relied on its security for internal communication and organisation of on-the-ground collective action; were organised in small private groups and large public groups to enable collective action; adopted tactics and technologies that enable pseudonymity; and developed a variety of strategies to detect compromises and to achieve forms of forward secrecy and post-compromise security when group members were (presumed) arrested. We further show how group administrators had assumed the roles of leaders in these 'leaderless' protests and were critical to collective protest efforts.

1 Introduction

Large-scale urban protests offer a rich environment to study information security needs and practices among groups of higher-risk users by relying on a diverse set of digital communication platforms, strategies and tactics, and by their sheer size. In this work, we study the Anti-Extradition Law Amendment Bill (Anti-ELAB) protests in Hong Kong, where most activities and interactions map onto some form of digital communication. The use of different communication platforms as an integral part of the protests has already been documented in various media reports, including: large chat groups on platforms such as Telegram, protest-specific forums on the Reddit-like platform LIHKG, practices of doxxing as well as live protest maps such as HKmap.live to identify police positions [15, 16, 78, 99]. Recent scholarship has also highlighted the significance of digital technology to the Anti-ELAB protests. For example, "novel uses" of communication technology by Anti-ELAB protesters led them to form ad hoc and networked "pop-up" protests, creating a new form of a "smart mob" facilitated by digital technology [104]. Platforms such as Telegram and LIHKG worked to mobilise and establish a sense of community among young activists [87] and created a "symbiotic network" of protesters [61]. Social media was used to maintain "protest potential" over time [68].

To design and build secure communication technologies that meet the needs of participants in large-scale protest movements, it is critical that designers and technologists understand protesters' specific security concerns, notions, practices and perceptions. There is also a need to understand the existing use of secure and appropriation of insecure communication tools within such protest groups, where they fail and where they succeed. Existing qualitative studies have explored security practices of different groups of higher-risk users, e.g. [23, 24, 29, 33, 37, 42, 70, 74, 75, 94], but none to our knowledge have studied such practices within large-scale urban protests.

The Anti-ELAB protests, while specific in nature like any other local protest movement, provide ample material for a case study. This is not only for the features already outlined above – urban, large-scale, digitalised – but also because of the place these protests take in the imagination of protest movements across the globe. The perceived analogue and digital tactics developed in Hong Kong have been imitated by protesters elsewhere, often with a direct reference, see e.g. [21, 49, 84].

Contributions. We develop a grounded understanding of (perceived and actual) security needs and practices among Anti-ELAB protesters through in-depth, semi-structured interviews with 11 participants from Hong Kong. Through an inductive analysis of these interviews, research findings were synthesised into five main categories. We outline these in Section 5 – the tools used by Anti-ELAB protesters and the reasons for their adoption (Section 5.1), the role these tools play for the organisation of these protests (Section 5.2), the tactics used to detect and mitigate compromises through arrests (Section 5.3), the practices adopted to work around limitations of the tools relied upon (Section 5.4) and the routes and negotiations through which protesters arrive at their understanding

and practice of security (Section 5.5) – before bringing these into conversation with information security scholarship in Section 6, where we also identify open research questions, and concluding in Section 7.

2 Related Work

We position our research within studies on digital communication technology use by participants of large protest movements, including existing work on the Anti-ELAB protests to establish pre-existing understanding of their technology use, as well as scholarly work on higher-risk users.

2.1 Large-scale protests and digital communication

The importance of digital communication technology in large-scale protests is well documented in the social science literature, focusing in particular on the significant contribution of social media platforms to the mobilisation of social movements [18, 25, 31, 32, 66, 73, 77, 92, 112]. They also highlight the critical role that digital media play in the organisation and coordination of large-scale protests, e.g. Occupy Wall Street and the Arab Spring [5, 34, 48, 58, 81, 105, 109]. Yet, there is consensus in the literature that while the ability to form online networks can support mobilisation and organisation efforts, it is neither the sole driver nor the underlying cause.

Scholars also note how digital communication technology enables new networks and movement formations. For example, Bennett and Segerberg [12] describe a form of protest movements not reliant on resourceful organisations, but driven by personal online content and communications – what they call "connective action". Others, e.g. [18, 58, 73], highlight how digital technology enables the formation of decentralised networks among groups in different locations, through collective action. These movements are able to attract large numbers of participants, partly because they are supported by digital infrastructures [67]. Studies have also suggested that people "self-mobilise" online before taking part in protests [44, 65, 95]. Finally, digital technologies are often used to facilitate on-the-ground organisation, information sharing and communication between protesters – what Treré [106, 107] calls "backstage activism".

Messaging applications. Some studies explore the use of messaging applications in distinct resistance movements and protest environments. For example, Uwalaka et al. [110] considered the use of WhatsApp in the 2012 Occupy Nigeria protest, Gil de Zúñiga et al. [119] and Valeriani and Vaccari [111] studied messaging applications in activism and political organisations, while Treré [107] showed how WhatsApp is used for everyday activities and organisation by protesters in Spain and Mexico. Similarly, Haciyakupoglu and Zhang [40] found that in the Gezi Protests in Turkey protesters relied especially on WhatsApp to circulate information within the protest area. Messaging applications have also been linked to the spreading of rumours and incitement to violence. For example, Mukherjee [79] explored the use of WhatsApp in mob lynchings in India and Arun [8] linked the spreading of rumours via WhatsApp to them. Tracking and hacking on digital communication platforms are also used by private and state actors to counter opposition movements and to suppress dissent [63, 76].

While such prior works do not consider (information) security in particular, they provide broader context and in some cases surface security-related findings. For example, the importance of trust in information, technology and social media networks is explored in [40, 67] and Tsui [108] studies digital technology use and protection from state surveillance efforts, while Sowers and Toensing [96] engage with wider security concerns such as threats to protesters from authoritarian and violent regimes.

2.2 Anti-ELAB protests

The protests responded to the Hong Kong Government's attempt to pass an Extradition Law Amendment Bill [64, 69]. Hundreds of thousands of people took to the streets, where networked groups of protesters organised mass rallies and strikes, boycotted pro-Beijing businesses, barricaded streets, stormed public buildings including the Legislative Council Complex, occupied traffic hubs and seized university campuses [47]. Recent studies have emphasised the centrality of digital and mobile communication technology to facilitate these large, dynamic and highly mobile protest activities; with tactics often referred to as "be water" and "blossom everywhere" [41]. Such tactics meant that the protests emerged from the ground up among activist networks in a nonhierarchical, diversified fashion, relying on spontaneous initiatives rather than top-down leadership and organisation. In general, this served two purposes. While it provided protection from prosecution of individual protesters and police detection, it gave rise to fluid, horizontal communication within and between dispersed groups of protesters [47]. These tactics were partly rooted in protesters' experiences from the 2014 Umbrella Movement in Hong Kong, where high-profiled protesters were arrested and imprisoned, and which were also supported by digital modes of participation that enabled, for example, real-time coordination of "improvisatory acts" [67].

The Anti-ELAB protests are widely considered to have been "innovative" in their tactics, particularly the interaction between "front line" protesters and others. A "frontliner", roughly, is someone engaging in activities that risk direct confrontation with law enforcement [21]. An example of a collaboration between "frontliners" and others are ride sharing schemes where car owners picked up "frontliners" to transport them out of the protest area because public transport was deemed unsafe or shut down [117]. These schemes were run via public online groups that connected protesters with drivers.

Existing scholarship reveals little about the security consid-

erations of Anti-ELAB protesters. Ting [104, p.363] notes that networked protesters used "encrypted messaging app Telegram and mass Airdrops over Bluetooth" to coordinate protest activities, and that WhatsApp and Signal were used to share protest information and to request supplies. Ku [87] points to the mobilisation of Hong Kong youth activists through Telegram and the Reddit-like forum LIHKG, while Kow et al. [61] show how "hundreds of groups" on these two platforms were used to mobilise the protests through polls and the ability to act anonymously. Importantly, however, none of these studies engaged with protesters, but relied solely on interpretative analyses of social media posts, forum posts and/or wider discourses.

2.3 Higher-risk users and secure communication

Looking beyond large-scale protests, our research ties in with other qualitative works exploring the security concerns of higher-risk users. The use of secure messaging by higher-risk users is considered in [33, 42]. Through interviews with human rights activists and secure messaging application developers, this work outlines common and diverging privacy and security concerns among these groups. They found that while developers aim to cater to higher-risk users, the (perceived) security needs of these groups of users are not well understood and thus not well served. Similarly, in [7] the authors discuss the divide between activists and technologists. They advocate that "security engineers [...] step into the language of collective action within a political project" to produce solutions that cater to the decidedly collective needs of activists and contrast this with a prevalent practice where "in the absence of far away users under threat, designers can invoke them at will and imagine their needs" [7].

The security needs of marginalised groups have received renewed attention from information security academics due to an invited talk by Seny Kamara at CRYPTO 2020 [57, 80]. In this talk, Kamara characterises "Crypto for the People" as "concerned with fighting oppression & violence from Law Enforcement (Police, FBI, ICE), from social hierarchies and norms, from domestic terrorists" [57] and contrasts it with a libertarian-inspired concern for personal freedoms. More broadly, studies have explored security for civil society groups [91], the security and privacy needs of journalists [71, 74, 75], privacy concerns among transgender people [70], protection practices by Sudanese activists [29], fundamental security challenges experienced by refugees [23, 24, 55, 94] as well as undocumented migrants [37]. Like many of these prior works, our work suggests that the population we study has distinct (information) security needs that must be understood in order to design security technologies that meet those needs.

3 Preliminaries on technologies

LIHKG is a Reddit-like forum that allows posts only from users with email addresses originating in Hong Kong (cf. [87]). **Signal** and **WhatsApp** are messaging applications that use phone numbers as contact handles and perform end-to-end encryption by default on all chats. Both applications support one-to-one chats as well as private group chats of up to 1,000 and 256 users respectively. **Telegram** is a messaging application that offers the option of end-to-end encryption for one-to-one chats only and supports public and private groups of size up to 200,000 as well as public channels with an unlimited number of subscribers. Telegram requires a phone number for registration but allows this to be hidden from other users. **Facebook Messenger** is a chat service connected to Facebook, offering optional end-to-end encryption. On the technology level, Telegram makes roughly the same security promises as Facebook Messenger with respect to confidentiality – with its bespoke MTProto protocol taking the role that TLS plays for Facebook – but it makes it easier to adopt a pseudonym.

Signal and Telegram secret chats allow users to send *disappearing* messages which are deleted by the sending and receiving application after a certain time has passed (five seconds to one week). WhatsApp has recently enabled this option but has a fixed timer of one week. Telegram also supports *scheduled* messages to be sent at a later date and time, before which the sending of the message can be cancelled.[1] Further, Telegram allows a user in a one-to-one chat to *delete* messages for the other party, and a group administrator to delete messages for all group members. Neither WhatsApp nor Signal used to support this feature.[2] Telegram supports conducting anonymous *polls* in groups and channels.

Life360 is an application that allows remote monitoring of a phone – e.g. location, remaining battery – that describes itself as a *"family safety service"* [72] but is mostly known for being invasive [82]. WhatsApp and Telegram also support *live location sharing* with another user for a period of time.

4 Methodology

In this section, we outline our methodology, which is based on a qualitative research design and a grounded approach [19, 45], informed by existing social movement research (see e.g. [13]).

4.1 Semi-structured interviews

Semi-structured interviews were chosen due to their exploratory nature; they are sufficiently structured to provide

[1] The messages are scheduled on the server and thus will be sent even if the user goes offline afterwards.

[2] As of January 2021, Signal includes limited support for message deletion for everyone (only the sender can delete their own messages, within three hours of sending) [93], but this was not the case when the interviews were conducted. WhatsApp now supports the same feature with a time limit of one hour.

consistency across interviews and to address particular research questions, while leaving space for participants to offer new meaning to the topics (see e.g. [35]).

Interview process. Informed by a topic guide, the interviews explored the use of communication technology within the protest environment and how protesters' security needs and practices shaped this use. Each interview covered topics such as communication technology use in Hong Kong, including specific platforms and applications as well as security concerns related to this technology use. The first two topics covered in the interviews deliberately did not focus on security, as it was important not to 'force' a security angle. However, all participants mentioned specific security concerns related to their use of technology before we asked about them. This is not surprising, since information provided to participants prior to the interviews included information about the broader research focus and the composition of the research team. Moreover, the adversarial context foregrounded security concerns. Interview questions were intentionally broad to ensure that the research remained exploratory. This is an essential aspect of qualitative research, which works in the context of discovery and therefore emphasises openness and depth. The interviews were conducted by one member of the research team, between December 2019 and July 2020, as outlined in Table 1. Interviews were conducted remotely in English.

Participants and recruitment. 11 participants from Hong Kong (P0-P10), all of whom had either primary or secondary experience of the protests, were recruited. All participants had attended at least one Anti-ELAB protest and were all members of protest-related online groups. The distinction between 'primary' and 'secondary' denotes front-line protest experience. Participants self-reported as 'only' having secondary experience, because they had not been on the front line of a protest and were therefore less likely to have direct confrontation with law enforcement, while participants with primary experience had.

Table 1: Participants & Interviews

Participants		**Interview**		
ID	*Experience*	*Duration*	*Medium*	*Timing*
P0	Primary	82 minutes	Audio	December 2019
P1	Primary	43 minutes	Audio	December 2019
P2	Primary	64 minutes	Audio	February 2020
P3	Primary	51 minutes	Video	April 2020
P4	Secondary	47 minutes	Audio	April 2020
P5	Secondary	39 minutes	Video	June 2020
P6	Secondary	62 minutes	Video	June 2020
P7	Primary	73 minutes	Audio	June 2020
P8	Secondary	53 minutes	Video	June 2020
P9	Primary	87 minutes	Audio	June 2020
P10	Primary	46 minutes	Audio	July 2020

We categorise participants' protest experience as *primary* or *secondary*, with the former defined as having been on the protest 'front line'.

The protection of participants was our priority at all stages of the research. Initially, we only contacted publicly-known figures in Hong Kong, which led to three initial interviews. We then reached out to potential participants through two local gatekeepers,[3] who shared our contact details and a participant information sheet (PIS) with potential participants. The PIS outlined what participation would involve and how we would protect participant information. Gatekeepers were not involved in our communication with participants and whether someone decided to participate was not shared with them.

No specific selection or exclusion criteria were used to target individuals except for their primary or secondary involvement in the Anti-ELAB protests. However, this was by no means a straightforward recruitment process. We contacted more than 60 individuals linked to the protests and recruited 11. There are a number of reasons for this. First, the sensitive nature of the research and the importance of anonymity for protesters made it difficult to identify and recruit individuals with relevant protest experience. Second, parts of the research coincided with China passing a new national security law for Hong Kong, which also imposes restrictions on engaging with "external elements" [90]. Thus, many of our contacts declined to participate for safety reasons. Third, COVID-19 meant that travel to Hong Kong to engage with protesters was not an option. Hence, all engagements were carried out online.

Human subjects and ethics. All of our activities were approved for self-certification through our institution's Research Ethics Committee before the start of the research. Given the high-risk environment, and since our priority was to protect participants, we made sure to design our study in a way that minimised the collection of personally identifiable information. We recommended encrypted and ephemeral modes of communication, but followed participants' preferences, while using burner devices and anonymous accounts on our end to limit potential attack surfaces. Interviews were carried out by one researcher and were not audio recorded. With explicit consent from participants, extensive interview notes – verbatim where possible – were captured by the researcher. These were transcribed and stored on an encrypted hard drive.[4] To minimise risks to participants and researchers, we compartmentalised internally and only the researcher who carried out and transcribed the interviews has access to the raw data. Participants were not required to make their names known to us and we did not record any personal details in our interview notes. We do not report demographic information such as age or gender, nor do we report participant locations or their employment status. This is to protect their anonymity. Finally, participants were not compensated for taking part.

4.2 Data analysis

Interviews were analysed through an inductive analytical process, where the same (one) researcher coded the data through

[3] See e.g. [43, Ch.3] for a discussion on the use of gatekeepers for access.
[4] Transcripts are retained for one year after publication and then destroyed.

three coding cycles using NVivo 12 [51]. The first cycle used open coding and produced a range of descriptive codes, which were grouped in the second cycle to produce axial codes [88]. In the third coding cycle, the core variables in the data were identified and selective codes were produced and grouped into categories [85]. This form of analysis is employed to identify and analyse patterns across a qualitative data set, rather than within a particular data item, such as an individual interview. At the final stage of the analysis, technological implications were explored by the entire research team.

Limitations. A number of limitations should be taken into account when interpreting our findings. First, our study was limited by the difficulties we experienced in engaging participants in our research, as outlined in Section 4.1, and research findings might have captured other practices if further interviews had been conducted. Yet, the semi-structured nature of the interviews was chosen to provide depth rather than scale. Moreover, the analysis suggests that coding saturation was reached. Second, conducting interviews online limited the researcher's ability to observe the participants' physical settings, which might have affected their ability to speak freely. Third, some protesters, who declined to participate, might have been particularly concerned about security. Fourth, while participants spoke fluent English, it might have been possible to recruit a broader selection of participants if interviews had been conducted with the assistance of a translator.

Finally, there is an inherent bias in interview-based research, particularly when it concerns security or technology questions, given that participants self-select to take part. Some contacts decided against participation because they did not feel that they knew enough about the technologies they were using. This limitation is not unique to this study, but mirrors other technology-focused interview-based studies; they are inherently biased towards the more tech-savvy end of the population being studied, such as security trainers or attendees of IT security trainings. Future work should consider adopting ethnographic methods of inquiry to overcome this limitation.

5 Research findings

Our research findings are structured into five subsections: Section 5.1 focuses on the technologies used by protesters and why, Section 5.2 shows how these technologies interact with the social organisation of the protests, Section 5.3 discusses tactics for detecting and reacting to arrests, Section 5.4 shows how protesters address the limitations of the technologies they rely on, and Section 5.5 focuses on how and from where protesters develop ideas about their security.

5.1 Tools

Internal communication between Anti-ELAB protesters was mainly done through two messaging applications: Telegram (predominantly) and WhatsApp, with most protesters joining dedicated protest-related groups on both applications.

Telegram was used by all participants and dominated our findings. One participant summarised Telegram as *"the most useful platform, followed by WhatsApp"* (P0), while another expanded: *"For communication and organisation, most people use Telegram"* (P6). Participants observed that its popularity in the protests was based on three conditions: (1) its widespread adoption prior to the protests, (2) its security, which was perceived to be better than any other messaging application and (3) the ability to form both large and small groups. Telegram's polling feature emerged as another reason for adoption as well as various of its features used to monitor fellow protesters for arrest, as discussed in Section 5.3. Participants understood Telegram to give them the *"most security"* in group chats (P0). As explained by one participant: *"We have a group on WhatsApp and another one on Telegram, but we use the one on Telegram to talk about our actions [...], because we think Telegram is more secure"* (P9). One participant (P5) noted that, although end-to-end encryption was not the default setting in Telegram group chats, this could be enabled. This is incorrect (see Section 6.3) and demonstrates how an incomplete or, as in this example, incorrect understanding of security might shape participant perceptions.

WhatsApp was also used by the majority of participants in our study and they assumed that this would be the case for others too: *"most protesters use WhatsApp too, yes definitely"* (P3). Yet, WhatsApp was seen to be less suitable compared to Telegram because it only allows for groups of up to 256 members.

While *Signal* was brought up by several participants without prompting, our data suggests that it has not seen any significant adoption among Hong Kong protesters. Participants highlighted the discrepancy between what they perceived as their security needs and what is offered by Signal. First, the need to provide a phone number was seen to conflict with the need for anonymity to avoid police detection: *"the reason we don't use Signal is because Signal requires that you know the telephone number of the other people if you want to make a contact"* (P7) and *"The thing is, people in Hong Kong cover their faces when they go out to protest. They want to be anonymous. So, if you have to then give your phone number, it doesn't make sense"* (P7).[5] When asked whether they would consider using burner SIM cards to use Signal, they responded that the benefits would not outweigh the risks. Second, the function of being able to delete messages sent by other group members was key for protesters: *"You cannot tell people to use Signal instead of Telegram, because that's not realistic and also Signal is horrible at other things that the protesters need. For example, you cannot control what happens to your messages once you have sent them. You can just use disappearing messages"* (P6). Thus, participants in our

[5] Anti-ELAB protesters defied the ban on wearing face masks that was introduced in Hong Kong in October 2019 [17].

study compared the security offered by Signal to Telegram – not to WhatsApp – when making decisions about which tools to use.

While WhatsApp also requires phone numbers, it was already widely used by participants before the protests and they felt confident and, as a result, secure using a tool with which they were already familiar. Where Telegram catered to their need for anonymity in large group chats, WhatsApp was used for small close-knit groups, where anonymity was not a security need. Hence, Signal was not seen to provide them with additional security or required key functionality.

5.2 Social organisation

Our work speaks to the utility of groups on messaging applications for on-the-ground protest organisation enabling collective practices, strategies and tactics – and to related security requirements. Here, we discuss such practices and show how different types of groups, characterised by their size, imply different, at times opposing, security requirements.

5.2.1 Group types. Two types of groups were identified in the data: large Telegram groups, sometimes with 2,000, 20,000 and 50,000 members and small(er) groups on both Telegram and WhatsApp. The former comprised public groups set up to disseminate protest information across large networks, facilitate collective decision making and reach and connect disparate groups. The latter were formed around more or less close-knit groups of protesters.

All participants in our study were members of several Telegram groups; some small groups, made up of people they had met during the protests, and some large groups, which they predominantly used for information-gathering purposes. This divide also mirrors the division between participants' protest experience; those with only secondary experience had never been part of small protest groups, but were in several large public Telegram groups. Participants with primary protest experience were members of both types of groups. All participants, regardless of protest experience, gave examples of how they knew that the large Telegram groups were infiltrated by e.g. local police officers, who monitored the groups to gather information about protesters and protest strategies. Several participants also reported deliberate attempts to undermine the protest efforts in these groups by presumed infiltrators. While there was general consensus among participants that the disruption caused by these infiltrators was minimal, it highlights an important aspect of big group chats: all participants accepted that confidentiality could not be achieved in these large groups, while they assumed that it could be achieved in the smaller groups. However, large groups were essential for the successful organisation of protest activities because of their scale and reach – and crucial for the collective actions that they facilitated, such as joint decision making.

For all participants with primary protest experience, being able to organise quickly and securely was the key motivating factor behind having smaller rather than larger groups. The large groups were run by dedicated administrators (see Section 5.2.4), while the small groups were formed *"quite organically and not that organised"* (P5). Each small group, however, had its own identity, its own utility. One participant explained this by drawing on two groups, one with 26 members on Telegram and another one with six members on WhatsApp: *"there are still some differences between those 26, because I met six of them and formed a small team. But the other 20 joined later. So, actually, those 20, I haven't met them before, face-to-face. We have the WhatsApp group, only the six of us. And on Telegram we have the 26"* (P2).

5.2.2 Strategies and tactics. The importance of secure messaging applications for protesters has already been articulated in previous works, e.g. [33, 42, 107, 119]. In the Anti-ELAB protests, such applications more specifically cater to the particular strategies and tactics employed by protesters: a flat structure, mobile, dynamic and large-scale in nature. All participants in our study explained how the ability to collectively decide on strategies and tactics in real time across large and geographically dispersed protest sites was essential to the success of the protests. One participant articulated how Telegram provided a *"safe online space"* to collectively decide specific actions: *"we use Telegram to talk about our actions, our equipment, our strategies, our tactics"* (P2). Another participant spoke about how Telegram enabled immediacy, which was needed when tactics had to be altered during a protest: *"during the protests themselves, the information is more related to strategy, like, what to do right now"* (P5). Both quotes highlight the sense of urgency felt by participants when talking about sharing tactical information during protest actions.

Several other participants expressed a sense of information overload given the volume of information being shared during protests. This often made it difficult for them to keep up with evolving protest tactics. One participant noted: *"When protests are actually taking place, the groups are much more active, there's information all the time and it's difficult [. . .] to know what the strategy is"* (P9). Such statements exemplify the challenges experienced by protesters when faced with multi-directional and extensive information in both adversarial and highly digitalised environments: *"it's hard to keep track of stuff"* (P10). All participants with primary protest experience spoke of how they would have to make tactical decisions within seconds when receiving information about police locations or new gathering points. For many, this meant deciding which groups to *"keep open and which to close"* (P7) while participating in protest activities, hence, limiting the information they would have to digest.

5.2.3 Collective decision making. Protests are by their very nature a collective endeavour and the mobilisation of protesters has been the topic of many recent works, as identified in Section 2.1. However, beyond mobilisation, our data reveals how Telegram and LIHKG were used to make collective decisions about protest tactics, in real time.

Several participants in our study exemplified how large Telegram groups were used to vote on *"the next move"*, as explained by P7, while LIHKG was used to vote and decide on broader protest strategies at the start of the protests. *"This forum called LIHKG. We used it for strategy and stuff. Like in Reddit, people can vote [. . .] And we used it because you can only register with a Hong Kong email provider"* (P9). These features – collective and limited to people with a Hong Kong email account – made LIHKG a central platform early on in the protests. One participant suggested that it enabled *"nuanced discussions about strategy and to vote on strategy"* (P5). Yet, many participants noted that, over time, the organisation of on-the-ground actions *"couldn't be done on the forum because the police is monitoring it"* (P9). Thus, for real-time voting on tactical moves during protest actions, protesters had moved to Telegram groups, where polls on, for example, *"where to go next"* (P10) often received several thousand votes. While all participants in our study also assumed police monitoring of the public Telegram groups, the speed with which collective decisions could be executed made police infiltration less of a concern. Forums were, on the other hand, generally seen to be slow and not suitable for live protest action.

One participant explained how the voting worked best when only a few options were given, enabling protesters to make a *"simple choice between A or B"* (P3). However, based on our data, we see that the option with the most votes is rarely followed by everyone. Given the anonymous nature of these groups and of the polls – and since anonymity was a key security need for Anti-ELAB protesters – it is unclear who votes in these polls. The scale of these groups was, however, critical for the success of the protests for two main reasons: it established a strong sense of collective decision making which, in turn, meant that no single person was seen to be publicly leading the protests. For the protesters, this had a security function as well, as it was seen to spread the risk of arrest to several thousands of people; to everyone who voted.

5.2.4 Group administrators. The centrality of protest groups on messaging applications meant that group administrators occupied key positions in the protests. Without public leaders, our data suggests that group administrators were seen as the leaders of the protests. While not directly articulated by the participants in our study, many of them spoke to the multiple and critical roles performed by group administrators and the trust that protesters placed in them. Importantly, however, group administrators remained anonymous leaders, hiding their identity to avoid police detection. Moreover, most groups had several administrators to *"spread the risk [for the group] to more than one person if one admin is compromised"* (P9), allowing non-compromised group administrators to revoke the administrator capabilities of those compromised. The same administrator also often managed several groups at the same time through different accounts.

Our data contains several examples that support the interpretation that administrators took the role of leaders. One participant noted: *"We have groups for voluntary medical support, and we have many groups for legal support. So, the whole protest, without leaders, is organised by these group administrators"* (P9). This mirrors how many participants experienced the protests themselves: as a decentralised movement, with *"many people who lead but no organisation"* (P3) or *"flat but not leaderless"* (P2).

To illustrate the central role of administrators, we use an example that was recounted by all participants in our study: a voluntary ride-sharing scheme. This was critical to get protesters ("frontliners" in particular) to/from protest sites, as using public transport was *"too dangerous for protesters because the police go to public transport to attack and arrest people"* (P3). However, many participants noted that the scheme required protesters to trust the administrators of the groups through which the scheme was run and their vetting procedures, which relied on drivers sharing their licence details with the group administrator(s). This was a way for them *"to verify the driver's identity before referring them to the protesters"* (P2). When a protester requested a driver through the group, the administrator would *"link up the car/driver and me as a protester. We don't know the driver or the administrator, but we know the licence number"* (P7). Some participants noted that while administrators would try to verify the driver's identity before referring them to protesters, they knew of several examples of undercover police officers pretending to be drivers, resulting in arrests. Still, participants with primary protest experience had all used this scheme and said, in different ways, that they had *no choice* but to trust.

5.2.5 Onboarding practices. The practice of establishing close-knit groups on Telegram and WhatsApp led to a number of security constraints for protesters, which centred on the need to establish trust within highly digitalised and adversarial environments. All participants with primary protest experience noted how their groups had developed particular onboarding practices rooted in interactions at sites of protests. This was seen as necessary to verify the identity of any newcomer to the group and ensure trust among group members. Based on the experiences of the participants in our study, specific onboarding practices were adopted for both Telegram and WhatsApp groups with between five and 30 members.

Our data shows how small close-knit groups were formed around protesters who had met face-to-face during the protests *"before moving the connection online"* (P4), as *"seeing each other and standing on the front line together is very important for trust"* (P10). These trust bonds were described to be established through shared aspirations and were seen to be key for the success of the protests as they enabled affinity groups to form and carry out essential tasks, e.g. provide legal or first aid. This was supported by another participant, who noted that it was important for their group that any new members supported their faction: *"So we see them in person first and we then also know that they are chanting the right slogan"* (P9). Participants also explained how offline connections would

only be moved online once rapport had been established with new group members. Our data suggests that, for most groups, this form of gradual onboarding to establish trust sometimes took weeks and sometimes months.

We unpack this collective process by using an example given by one participant, who belonged to two small affinity groups. They explained: *"First, we have to meet them face-to-face. It's not that you just meet them and then add them, it's about values and beliefs and aspirations. We want those newcomers to work with us in the field several times first. If they share the same beliefs and aspirations, they can officially join our Telegram group"* (P0). For the close-knit groups, where specific protest activities related to the group would be discussed (what protesters deemed *"sensitive information"*), all existing group members would have to meet any new group members before they would be allowed to join.

Our data contains some examples of specific onboarding processes where some group members had been unable to meet a new group member. This would then become a negotiation between existing group members: *"someone in the group will say 'I know a person who might be able to contribute to this group', and there will then be a short discussion and then a decision"* (P3). Participants noted that while this was not *"bullet proof"* (P10), it was also important for them – and for the success of the protests – to accept group members who they thought would be able to contribute to their efforts. However, this form of onboarding was accompanied by a level of distrust for some participants, who would insist on meeting all potential group members before accepting them into the group: *"I would want to meet all group members in person first, before accepting them"* (P1). As expressed by another participant: *" Sometimes you have to make a choice, even if you haven't got enough manpower, you only recruit people who you trust"* (P10). The main concern was articulated as *"potential infiltration of police"* (P7). This was a common worry expressed by participants and was connected to their experiences with large Telegram groups, where police infiltration was explained to have led to several arrests.

5.3 Indicators of compromise

Our data demonstrates that the threat of arrest during a protest and the subsequent compromise of the arrestee's close-knit affinity group was a key concern for participants. Our data shows that different protest groups adopted subtly different approaches to monitoring each other while attending protests. Our data also suggests that this was a widely adopted collective (security) practice for Anti-ELAB protest groups.

Our data contains three approaches to monitoring: the use of specific monitoring applications, scheduled messages or regular messages. The use of specific live-tracking applications was practised by several participants and comprised a system whereby when some group members went onto the street, the rest of the group would be responsible for monitoring their whereabouts using WhatsApp or Life360. Some participants explained how they would use both applications simultaneously to ensure that they would be able to receive constant updates. This was seen as particularly useful to determine whether a group member had been arrested: *"There are some signals that tell me that the person got arrested. For instance on the live location, if they disappear from the map then I know something is wrong [. . .] if I know they have battery and suddenly disappear then I can call them. If no-one picks up the phone for a long time and we can't find them in the field, then we will track their last location. And then we know whether they have been arrested"* (P1).

Another participant detailed their group's approach to live monitoring, which relied on regular messages: *"If my friends go out in the protest, I'll stay up and every hour I'll text and ask 'are you safe?' And if they don't respond within two-three hours I'll assume that they are arrested"* (P3). The same participant reported that *"there's a feature in Telegram that allows you to periodically send out a message. So, it does something automatically periodically – so these pings are exchanged among a group and if you see that someone isn't responding to the ping, then probably something bad has happened"* (P3).[6] Another group used timed or scheduled messages to alert group members should their phone be inactive for a period of time: *"we use timed messages, so others know that if they receive the message, I'm probably arrested"* (P9). That is, protesters would schedule a message to be sent later and would cancel this scheduled message once they returned from the site of protest. If they failed to cancel the message, this was taken as an indication of a problem.

Other participants gave similar accounts and noted that these practices had been systematised within many groups – and that groups had learned from each other – in response to a growing number of arrests. For them, being able to monitor each other was seen as a way *"to protect others when someone gets arrested and also to provide legal assistance"* (P3). For all participants in our study, this form of monitoring was important to protect and support group members in the event of arrest: first, by arranging for legal aid and, second, to control access to information about or related to other group members. It is for this reason that the ability to delete messages sent by any member in a group was seen as vital. In case of an arrest, the group administrator(s) were responsible for removing messages from the arrestee's device and to remove them from the group. This feature was seen as key: *"I can delete the messages for others, not only for myself"* (P7); as allowing them to *"control the conversation"* (P4) or to *"control what happens to your messages"* (P5) and to kick out anyone who had been arrested and to delete all group messages – *"so we can at least keep the others safe"* (P2).

Our data highlights a number of concerns and conflicts raised by participants in relation to such live monitoring prac-

[6] This is not a feature included in Telegram as described, but note that bots [102] may be used for this purpose as they allow to expand the functionality of the application when added to a chat.

tices. First, the concern that their live locations might become available to the police showing that they had *"committed crimes by being in locations they aren't meant to be"* (P7). Thus, this appropriation of consumer applications with unclear privacy guarantees illustrates the limitations of existing security technologies. Second, live monitoring through specific location-tracking applications was also seen to limit participants' control over access to data as it is not possible to delete the data in Life360 or WhatsApp: *"if a group member is arrested, the police can track the others via the app as we cannot delete for others"* (P2). More broadly, participants articulated how they would try out different technologies to find *"the best solution available"* (P5), but also know that these did not serve their security needs. We expand on this point in Section 5.5.

5.4 Limitations of technology

We present the additional practices adopted by protesters to address the limitations of the technologies they use. Protesters spread their identities across different accounts and devices to achieve a level of pseudonymity and a variety of low-tech tactics were adopted to handle congested networks.

5.4.1 Pseudonymity. All participants in our study spoke about how their involvement in the protests had heightened their focus on personal and information protection. For participants, particularly those with primary protest experience, any personal information was considered sensitive. In security terms, their (online) identity was closely tied to their protest activities, driving a growing need for pseudonymity: *"protesters make their profiles private, they use a separate SIM card, they use pseudonyms and so on"* (P6). Several participants explained how protesters had *"a separate phone when [they] go out and a separate SIM card"* (P4) and how they had *"another group with a different number which is attached to a different SIM card and completely isolated from the usual groups"* (P2). This separation between protest groups and phone numbers was seen as a key mechanism for protecting individual anonymity and to go undetected by the police: *"So, that's why we don't want to give out phone numbers, even with burner phones"* (P9). Another participant articulated how they, along with other group members, had several phones and other devices as well as several accounts on different applications. This is in addition to several protesters sharing one account, which was said to be done to ensure that others *"won't know they are not the same person"* (P10).

These desires to protect their identity and the identity of group members, combined with what many participants referred to as increasing surveillance measures by Hong Kong authorities, were articulated as causing a critical need for anonymity. This need was also linked to the popularity of Telegram as a protest tool in Hong Kong: *"I think Telegram is particularly good because it allows you to stay anonymous"* (P5). Yet, participants also noted how the *"move to Telegram"* had created a *"conflict between trust and anonymity"* (P9) because they were no longer able to *"look at people's Facebook profiles"* (P7) to establish their identity; a practice that was used extensively during the 2014 Umbrella Movement. Hence, online vetting of potential group members had become impossible.

5.4.2 Disconnected discontent. All participants with primary protest experience had also experienced being disconnected, due to network congestion, while taking part in protest activities. They explained how they had found alternative ways of communicating with other protesters. These took different forms.

First, some participants with primary protest experience articulated how they relied on interactions with other protesters in the street, which enabled them to develop and use hand signals to pass on messages: *"Sometimes it's just much easier just to wave or communicate using some hand gestures, when the network is down"* (P10). Participants gave specific examples of this form of non-verbal communication. They noted that hand signals were often used to communicate which supplies were needed on the front line: *"If you see someone doing a cutting motion with these two fingers [index and middle fingers] you know that scissors are needed"* (P9). Arms orbiting the head was said to indicate that helmets were needed on the front line (P7). Second, some participants spoke about how they would go to places with WiFi facilities to try to send messages during the protests. Yet, this approach was only adopted at critical points when they saw no other ways of communicating. Third, some participants noted how they would *"revert"* to using SMS, at times when they could not connect to the Internet. Exemplified here by one participant: *"there was a time when I was at [location] because of the protests and couldn't connect to a network for some reason and couldn't connect via Telegram or WhatsApp. So, we could only connect with the outside via SMS. Paid messages"* (P2).

Finally, most participants had heard about the mesh networking application Bridgefy (see [3]), which according to news reports saw a spike in downloads in Hong Kong in September 2019. However, none had successfully used it: *"it just doesn't work"* (P7).

These alternative approaches of connecting when the Internet is not available speaks to the disconnected needs of Anti-ELAB protesters. While Hong Kong authorities did not resort to shutting down the Internet, protesters experienced significant disruptions to their digital communications. These disruptions, which are a feature of the protests' large-scale nature – *"A million people just makes it impossible to communicate"* (P9) – render the technologies that protesters rely upon largely futile, at the height of protests.

5.5 Routes of security perceptions

We explore where Anti-ELAB protesters' notions and ideas about security and their own security needs have come from. In so doing, we first show how previous protest experience shapes protesters' practice of security and how the adoption of

messaging applications is a result of a change in security mindset among protesters. Second, we show how protesters with no or limited protest experience adopt the technologies and practices employed by more experienced protesters. It is worth noting, however, that our data reveals that participants with only secondary experience of the protests assumed greater adoption of applications such as Bridgefy and Signal than what was exemplified by participants with primary protest experience. This is not surprising given how (inter)national media outlets have reported on some of these technologies [60]. Yet, it is important to distinguish between actual and perceived adoption and requirements, and it points to the urgent need for secure technology designers to engage with the groups of users they seek to serve, as also noted in [7].

5.5.1 A shift in security mindset. Our data suggests a change in protesters' security mindset during the Anti-ELAB protests, with most participants highlighting a growing need for anonymity, due to heightened surveillance, and confidentiality, in relation to trusted and close-knit small groups. All but one participant with primary protest experience had also taken part in previous protests in Hong Kong and had experience of using technology within such protest environments. These participants compared their experiences in the current protests with those of the 2014 Umbrella Movement, where *"you basically had no access to the Internet as there was so much traffic and the network was super slow"* (P3) and *"most was organised over Facebook"* (P2). In addition to changes to technology, several participants highlighted how the protest environment had become increasingly adversarial: *"In the 2014 movement, things happened much more slowly [...] There was no conflict most of the time. But this is very different now"* (P9). Many participants noted that this had led to a shift in security mindset among protesters. While *"before June last year [2019], people would be gathering on Facebook"* (P6), *"just talk about about sensitive information on Facebook's messenger"* (P10) and *"not think about end-to-end encryption"* (P2), this had changed with what they described as an increase in police surveillance and arrests. This shift in mindset had led to a greater adoption of Telegram.

5.5.2 Collective information security. For Anti-ELAB protesters, as articulated by the participants in our study, information security is a collective endeavour. It is practised by individual protesters, who have their own security perceptions and needs, yet these are shaped by the security decisions of the group. At a high level, this is not surprising given the centrality of groups in these protests, the practice of voting on strategies and tactics, and the fact that not everyone holds the same security knowledge. It does, however, speak to how security is practised within groups.

It also demonstrates that, to be a group member, protesters have to buy into the security collectively decided for the group. One participant explained how they had tried to convince members of their group to switch to Signal after they had realised that *"people in other countries use Signal"* (P2). Yet, this had been unsuccessful as other group members preferred to keep the group on WhatsApp, as they were already familiar with this application and its (perceived) security. This led to them having to compromise their own security needs to be a group member. One participant said that they had changed their practices to be in line with other group members: *"I only started to use Telegram during these protests. I didn't use it before. I heard that Telegram is used by terrorists, because it is so secure. And it is used by my groups"* (P1). This participant accepted that they *"had to conform to be in the group"*. Participants explained how they had observed others *"change their security mindset"* to buy into the security of their group (P3).

Our data also contains several examples of how participants were either unsure about the level of protection offered by some of the technologies they used or knew that a particular application was not *"the most secure"* (P10). For example, one participant explained how they had accepted that they could not *"do everything to protect"* themselves (P9). This was reiterated by another participant: *"I do not know if Telegram or WhatsApp are safe to use or whether the Chinese government can listen in, but I use them because others use them"* (P7). Moreover, some participants had accepted that their security needs would not be met by the technologies they used but that they offered *"good enough"* security (P0).

Participants with less protest experience or who did not perceive themselves to be security conscious noted how they relied on other protesters for advice. At a group level, the security approaches and technologies adopted by one group would often be adopted by another group. This is evident from comments made by participants about how they would look to more established groups for security advice. Our observations about onboarding practices and live location monitoring also exemplify this point. First, onboarding processes adopted by groups were generally performed in similar ways. Second, live location monitoring was practised by all groups that included participants with primary protest experience. These subtly different approaches centred on only a few technological solutions and established practices.

6 Discussion

In this section, we reflect back our findings to information security scholarship, with a focus on cryptography.

6.1 Secure messaging

Telegram. The participants in our study reported Telegram as the predominant messaging application used by Anti-ELAB protesters. This finding is corroborated by media reports, e.g. [11], and corroborates prior work that established the use of Telegram by activists [33]. However, Telegram has received relatively little attention from the cryptographic community [54, 59] or information security research [1, 6, 98]. As

noted in [59], academic attention is focused on the Signal Protocol partly due to its strong security promises such as forward secrecy and post-compromise security. Indeed, even when Telegram is studied, its end-to-end encryption in secret chats is the focus, cf. [54,59]. This feature, however, has little impact on the actual security provided by Telegram in the use case considered here, since secret chats are one-to-one only. Group chats are secured at the transport layer by Telegram's bespoke but understudied MTProto protocol, which Telegram typically uses in place of TLS.[7] Telegram also implements a variety of features meant to support anonymity within groups, often in response to user demand [100, 101], which have not been rigorously examined. Our work suggests the study of MTProto and the anonymity guarantees of Telegram's group chats as pressing problems for future work.

Messaging Layer Security (MLS). Our findings support the decision by the MLS working group to support groups of up to 50,000 users [97]. On the other hand, our findings indicate diverging security goals for different types of groups, roughly characterised by their size, in the setting under consideration: anonymity of group members towards each other but no confidentiality in large groups forming one type, and another one being confidentiality and authentication in small, close-knit groups. Our data presents a use case where a hierarchy of permissions in groups is central and where out-of-band authentication of group members may be assumed, weakening the need to trust the Authentication Service as defined in [97]. MLS does not model group permissions at a cryptographic level but aims to be compatible with this use case when such restrictions are externally enforced. It is worth noting that MLS supports multiple devices per user, while our data presents the practice of multiple users sharing the same account. It is plausible, though, that this conceptual difference does not make a difference in practice on the MLS level.

6.2 Security notions

Compromise. In the literature, the notion of *forward secrecy* (FS) [38, 62] is understood as the protection of past messages in the event of a later compromise of an involved party and the notion of *post-compromise security* (PCS) [22, 28] as the protection of future messages some time after a (usually full state) compromise. Both of these security notions work with a persistent, global adversary of some form. Post-compromise security protects against an (ordinarily at some point passive) adversary after a compromise. Forward secrecy protects against an adversary that either passively observed the communication (weak FS) or even actively attacked it before the compromise.[8]

The compromise the participants in our study were most concerned about was during and after an arrest. Here, they were concerned with both forward secrecy (remote message deletion) and post-compromise security (excluding an arrestee from a group). However, their notions differed from those in the literature. First, a cryptographic scheme achieving forward secrecy would not achieve the notion of forward secrecy desired by the participants in our study as messages remained stored on the recipient's device.[9] That is, our participants assumed and aimed to protect against a compromise that reveals not only key material but also the entire chat history (stored on the phone). Second, a security goal of the participants in our study was to protect themselves during the compromise not just afterwards. As indicated in our research findings, there is a variety of behaviours attempting to detect and control compromise *as it happens*, including location monitoring, timed messages, revocation of administrator capabilities and message deletion for others, all done on behalf of the compromised person by the remaining group members (we discuss the resilience of these methods in Section 6.3). Critically, their notion of post-compromise security was at a group level (removing the compromised party) rather than for the compromised party.[10]

Overall, the adversary model of the participants in our study is both stronger (the adversary also compromises the chat history; protection against an adversary during a compromise is intended) and weaker (detectable) than those in the literature, i.e. the resulting security notions are incomparable.

Time and place. Implicit in our data is that security and access requirements change with time and place. Group members away from the front line are assumed to be relatively safe, compared to those on the front line facing immediate arrest. This suggests a partial solution for forward secrecy. Group membership could be restricted while out in the field – e.g. messages disappear faster, no access to the list of group members, only pseudonymous handles, no admin rights – with fuller access being restored using a secret-shared key afterwards.[11] More broadly, it suggests modelling the dynamic nature of access privileges over time and place.

Anonymity and authentication. The use of forums such as LIHKG and large public Telegram groups, combined with the desire to avoid being tracked, suggests a need for a different kind of communication platform. If infiltration is assumed, the focus shifts from protecting confidentiality to protecting identity. As our data shows, this focus on anonymity surfaces the question of how to establish trust. A number of proposals exist in the literature: Dissent [27] claims a "collective"

[7] In [33] it is incorrectly reported that group chats default to TLS.

[8] Social dimensions of targeted attacks (active) and mass surveillance (passive) are discussed e.g. in [39, 53, 57].

[9] Disappearing messages only provide a partial solution, leaving messages received within the expiration window exposed.

[10] It is worth noting that the grounding of authentication in offline interactions and the assumed detectability of a compromise provides a mechanism to achieve some form of post-compromise security in the more traditional sense out-of-band, possibly at the cost of replacing a burner phone and/or chat group.

[11] This would partially mirror the practice adopted by some business travellers to move their data across borders online to avoid confiscation at the border, the latter being a use case used to motivate PCS in [28].

approach to anonymous group messaging with accountability, Riposte [26] aims to provide a secure whistleblowing or microblogging platform that resists disruption and AnonRep [118] presents an anonymous reputation system for message boards. The systems vary in cryptographic assumptions, threat models as well as ability to scale, but none of them provide real-time messaging and are hence only suitable for public forums that are not time-sensitive. None of the cited works have moved beyond the prototype stage, and many open research questions remain in the area.

Closely related is the study of reputation systems, whether centralised [14, 36] or decentralised [9, 83], originally motivated by the information leakage in services such as eBay or Uber which utilise public user ratings. It is not immediately clear how such a system could be translated to the setting of user trustworthiness in anonymous messaging, but the emergence of crowdsourced services such as the voluntary car scheme reveals potentially more straightforward applications. Yet, the context in which reputation systems are reasoned about is largely limited to marketplaces and cryptocurrencies. Moreover, given the strong emphasis on collective or group action indicated by our data, it is an interesting open question where (if anywhere) group [20] or ring [86] signatures, the primitives often underlying reputation schemes, may productively be deployed. However, the high level of mutual trust required to operate in small affinity groups and the practice of sharing account credentials might make the functionalities of these primitives unnecessary.

Trusted third parties. Our data indicates that the Anti-ELAB protests rely heavily on trusted third parties. This is true in a technological sense, e.g. group chats are not end-to-end encrypted and facilitated by Telegram's servers, which are protected by geopolitics, i.e. the limited reach of the current adversary. This observation corroborates prior work on activists [33].

While this technological reliance might be an artefact of necessity – viable alternatives are absent – our data also shows that trusted third parties, in the form of anonymous group administrators, are a central feature of these 'decentralised' and 'leaderless' protests. The work of Azer et al. [10] highlights the significance of what they call "connective leadership" in digitally enabled and self-organised contemporary activism. Echoing this work, our findings illustrate how even 'leaderless' protests require leaders to connect protesters and protest groups. In the Anti-ELAB protests, due to their highly digitalised nature and experiences from the 2014 protests, group administrators act as connective leaders. This makes understanding their information security practices and needs a critical area of research for information security researchers, as the compromise of one of these administrators can have significant consequences, see e.g. [103]. This is particularly pertinent as large-scale protests around the globe adopt the strategies developed in these protests – their dynamic, mobile, digital and flat structure. On a technological level, recalling that the administration duties are often split between different individuals, and that the most prevalent form of compromise – arrest – may be detectable, MPC solutions, even in the efficient non-malicious setting, might suggest themselves.

6.3 Misconceptions

The participants in our study made security decisions based on specific functionality needs and explicitly formulated domain-specific security perceptions. However, our data reveals several mistakes in their perceptions of the security guarantees of the tools they relied on. Participants assumed that end-to-end encryption could be enabled in Telegram group chats, which is incorrect. The data also highlights that the ability to delete messages on other users' devices and to remove them from a group after an arrest drove the adoption of messaging platforms. Yet, these tactics assume that the compromised device continues to receive and process deletion requests; the more this tactic catches on and thus registers with the adversary, the more dubious this assumption becomes. Such misconceptions are not unique to our study. For example, several studies on usability, e.g. [52, 113], highlight user misconceptions and false mental models in relation to security. Other studies, e.g. [2, 30], also suggest that users find it difficult to understand the security of the applications they rely on and whether it fulfils their needs. For higher-risk users such misconceptions can have dire consequences for their safety, especially since the misconceptions identified in our study tended to overestimate the security guarantees given. Critically, however, our data highlights the negotiated and collective nature of adoption in this setting, in contrast to individual preferences foregrounded in previous work.

6.4 Collective security

Our findings speak to an understanding of information security that rests on collective practices, where security for the group is negotiated between group members and where individual security notions are shaped by those of the group. They show how Anti-ELAB protesters practised security to fulfil their own security needs as well as those of the group. Where these were in conflict, our findings suggest that protesters accepted the security approaches collectively decided for the group. Group membership was conditioned on realising specific security goals related to the Anti-ELAB context – anonymity in large public groups and confidentiality and authentication in small close-knit groups. Practices such as collective decision making to provide 'security in numbers' and tactical 'buy in' from group members substantiate the notion that, for the participants in our study, information security is a collective endeavour.

The idea of *collectivity* in information security is not novel, yet, research on group-level information security is sparse – and is largely limited to work on employee groups [4, 56] and socialising contexts [116]. Moreover, usable security scholarship generally considers security at an individual

level, as do user studies on messaging applications, see e.g. [1, 2, 30, 89, 114, 115]. While, collectively, these studies highlight a series of usability shortcomings of messaging applications, they do not consider the social environment within which these are used, nor do they consider collective security practices which dominated our study. They generally treat such shortcomings as technological problems and/or incomplete mental models among individual users, rather than also considering how users' wider social context and collective, negotiated practices shape their use of these technologies and how (in)secure they feel in doing so.

Our findings demonstrate that the particularities of *this* adversarial context, the Anti-ELAB protests, shaped participants' collective security needs and responses. Participants explained how social relations and trust were established at the protest sites rather than online and how this shaped their security practices, such as onboarding of new group members. In contrast to most usable security assumptions, our data shows that protesters go to great lengths to fulfil their security needs, conditioned on their adversarial setting and their group membership, but that such needs are not fulfilled by the technologies they rely on.

As we show in Section 2.3, other interview-based works on higher-risk users also emphasise the significance of the social context for the practice of information security. In bringing our findings into conversation with these studies, we note some high-level connections. For example, the participants in our study reported employing both technical and non-technical protection strategies, which has also been noted in recent studies on, e.g., journalists' use of security technology and related defensive practices [74] and political activists' "low tech" protection mechanisms in the context of the Sudanese Revolution [29]. Yet, while studies on other groups of higher-risk users, such as refugees and migrants, identify several cultural, social, economic and technological barriers that lead to unfulfilled security needs [37, 94], for the participants in our study, such barriers predominantly related to misconceptions about the security offered by the technology they relied on, the appropriation of insecure technology and their highly adversarial setting.

While it is possible to make some high-level connections between our findings and existing studies, the diversity of security concerns experienced by distinct groups and within specific contexts, requires grounded and situated research that is sensitive to this diversity. Moreover, our study, clearly illustrating how security is practised collectively among Anti-ELAB protesters, shows the critical need to situate technological security questions within the specific social contexts of groups, who share particular security goals. Thus, to understand collective security concerns and needs, future research should consider employing an ethnographic approach to "unearth what the group (under study) takes for granted" [46, p.551].

7 Conclusion

We conclude by summarising our key findings and by synthesising, with caution, requirements for (secure) messaging applications to serve the needs of protesters. Our interviews paint a diversified picture of group communication patterns, security needs and practices and they show how these are facilitated by a select few messaging applications and digital platforms.

Protesters rely heavily on Telegram and WhatsApp for their communication. Our findings illustrate how central these tools are for organising on the ground, by facilitating a collective approach to establish tactics, e.g. through anonymous polls, which was seen to provide both 'security in numbers' and 'buy in' for the chosen tactic. These decisions were made in groups of varying size and the administrators of these groups adopted the roles of leaders in these 'leaderless' and 'decentralised' protests. Overall, we found that these protests were organised in a mix of large public and small close-knit groups, with differing security requirements: anonymity within the group, on the one hand, and confidentiality and authentication, on the other. To bridge the conflicting requirements of anonymity and trust, participants reported a long, offline onboarding process before adding new members to a group.

The participants in our study developed tactics to detect compromise and to achieve some form of forward secrecy, i.e. protection of secrets against a later compromise. Group members monitored the movements of fellow group members to eliminate traces of the group chat from their phone in case of an arrest and to render legal aid. This explains the importance attributed to the ability to remotely delete messages on other people's devices. Participants adopted a variety of practices to address (perceived) shortcomings of digital communications and conflicting security needs. For example, to facilitate pseudonymity, compartmentalisation through the use of multiple devices and burner phones was widespread. Participants also reported how security decisions were collective, requiring group members to buy into the security practices of their group. This was a process fraught with conflict as differing security needs confronted each other.

For designers, several requirements on (secure) messaging applications emerge from our data: support for both (small) private and (large) public groups, the avoidance of phone numbers or other personally identifiable information and the ability of administrators to control messages and participation in groups. In particular, there is a clear distinction in security requirements for different types of groups: anonymity in large groups, confidentiality up to forward secrecy in small groups. In addition, going beyond strictly messaging, several features such as polls and live location sharing emerged as key enablers for participants. Participants also expressed a strong desire to be able to have control over their messages after sending them, such as on-demand remote message deletion.

However, we caution against taking this list of requirements

as a blueprint. First, our data only covers interviews with 11 participants. Second, these feature requests are informed by what existing technologies provide and thus do not necessarily represent the horizon of what is possible or desirable. Third, as we discuss above, the security guarantees provided by some of the employed tactics, particularly remote message deletion, are limited. Fourth, our data presents information security as a negotiated, conflict-laden and changing practice, suggesting that a universal solution may not exist.

Acknowledgements

We thank the participants for speaking to us and the gatekeepers for their assistance in establishing contact with participants. The research of Mareková was supported by the EPSRC and the UK Government as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/P009301/1).

References

[1] Abu-Salma, R., Krol, K., Parkin, S., Koh, V., Kwan, K., Mahboob, J., Traboulsi, Z., Sasse, M.A.: The security blanket of the chat world: An analytic evaluation and a user study of Telegram. Proceedings 2nd European Workshop on Usable Security (2017), http://dx.doi.org/10.14722/eurousec.2017.23006

[2] Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A., Smith, M.: Obstacles to the adoption of secure communication tools. In: 2017 IEEE Symposium on Security and Privacy. pp. 137–153. IEEE Computer Society Press (May 2017)

[3] Albrecht, M.R., Blasco, J., Jensen, R.B., Mareková, L.: Mesh messaging in large-scale protests: Breaking Bridgefy. Cryptology ePrint Archive, Report 2021/214 (2021), https://eprint.iacr.org/2021/214

[4] Albrechtsen, E., Hovden, J.: The information security digital divide between information security managers and users. Computers & Security 28(6), 476–490 (2009)

[5] AlSayyad, N., Guvenc, M.: Virtual uprisings: On the interaction of new social media, traditional media coverage and urban space during the 'Arab Spring'. Urban Studies 52(11), 2018–2034 (2015)

[6] Anglano, C., Canonico, M., Guazzone, M.: Forensic analysis of Telegram Messenger on Android smartphones. Digital Investigation 23, 31–49 (2017)

[7] Aouragh, M., Gürses, S., Rocha, J., Snelting, F.: FCJ-196 Let's first get things done! On division of labour and techno-political practices of delegation in times of crisis. The Fibreculture Journal (26), 209–238 (Dec 2015), http://dx.doi.org/10.15307/fcj.26.196.2015

[8] Arun, C.: On WhatsApp, rumours, lynchings, and the Indian government. Economic & Political Weekly 54(6) (2019)

[9] Azad, M.A., Bag, S., Hao, F.: PrivBox: Verifiable decentralized reputation system for online marketplaces. Future Gener. Comput. Syst. 89, 44–57 (2018)

[10] Azer, E., Harindranath, G., Zheng, Y.: Revisiting leadership in information and communication technology (ICT)-enabled activism: A study of Egypt's grassroots human rights groups. New Media & Society 21(5), 1141–1169 (2019)

[11] Banjo, S.: Hong Kong protests drive surge in Telegram chat app. https://web.archive.org/web/20201015094416/https://www.bloomberg.com/news/articles/2019-08-15/hong-kong-protests-drive-surge-in-popular-telegram-chat-app (Aug 2019)

[12] Bennett, W.L., Segerberg, A.: The logic of connective action: Digital media and the personalization of contentious politics. Information, communication & society 15(5), 739–768 (2012)

[13] Blee, K.M., Taylor, V.: Semi-structured interviewing in social movement research. Methods of social movement research 16, 92–117 (2002)

[14] Blömer, J., Juhnke, J., Kolb, C.: Anonymous and publicly linkable reputation systems. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 478–488. Springer, Heidelberg (Jan 2015)

[15] Blundy, E.C..R.: 'Bulletproof' China-backed doxxing site attacks Hong Kong's democracy activists. https://web.archive.org/web/20191101112411/https://www.hongkongfp.com/2019/11/01/bulletproof-china-backed-doxxing-site-attacks-hong-kongs-democracy-activists/ (Nov 2019)

[16] Borak, M.: We tested a messaging app used by Hong Kong protesters that works without an internet connection. http://web.archive.org/web/20191206182048/https://www.abacusnews.com/digital-life/we-tested-messaging-app-used-hong-kong-protesters-works-without-internet-connection/article/3025661 (Sep 2019)

[17] Bradsher, K., Victor, D.: Hong Kong leader invokes emergency powers to ban masks during protests. https://web.archive.org/web/20191004062033/https://www.nytimes.com/2019/10/04/world/asia/hong-kong-emergency-powers.html (Oct 2019)

[18] Castells, M.: Networks of outrage and hope: Social movements in the Internet age. John Wiley & Sons (2012)

[19] Charmaz, K.: Constructing grounded theory. SAGE (2014)

[20] Chaum, D., van Heyst, E.: Group signatures. In: Davies, D.W. (ed.) EUROCRYPT'91. LNCS, vol. 547, pp. 257–265. Springer, Heidelberg (Apr 1991)

[21] chuang: Welcome to the frontlines: Beyond violence and nonviolence. https://web.archive.org/web/20201009153811/http://chuangcn.org/2020/06/frontlines/ (Jun 2020)

[22] Cohn-Gordon, K., Cremers, C.J.F., Garratt, L.: On post-compromise security. In: IEEE 29th Computer Security Foundations Symposium, CSF 2016, Lisbon, Portugal, June 27 - July 1, 2016. pp. 164–178. IEEE Computer Society (2016)

[23] Coles-Kemp, L., Jensen, R.B.: Accessing a new land: Designing for a social conceptualisation of access. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2019)

[24] Coles-Kemp, L., Jensen, R.B., Talhouk, R.: In a new land: mobile phones, amplified pressures and reduced capabilities. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. pp. 1–13 (2018)

[25] Coopman, T.M.: Networks of dissent: Emergent forms in media based collective action. Critical studies in media communication 28(2), 153–172 (2011)

[26] Corrigan-Gibbs, H., Boneh, D., Mazières, D.: Riposte: An anonymous messaging system handling millions of users. In: IEEE S&P 2015 [50], pp. 321–338

[27] Corrigan-Gibbs, H., Ford, B.: Dissent: accountable anonymous group messaging. In: Al-Shaer, E., Keromytis, A.D., Shmatikov, V. (eds.) ACM CCS 2010. pp. 340–350. ACM Press (Oct 2010)

[28] Cremers, C., Hale, B., Kohbrok, K.: Efficient post-compromise security beyond one group. Cryptology ePrint Archive, Report 2019/477 (2019), https://eprint.iacr.org/2019/477

[29] Daffalla, A., Simko, L., Kohno, T., Bardas, A.G.: Defensive technology use by political activists during the Sudanese revolution. In: 2021 IEEE Symposium on Security and Privacy. IEEE Computer Society Press (2021)

[30] Dechand, S., Naiakshina, A., Danilova, A., Smith, M.: In encryption we don't trust: the effect of end-to-end encryption to the masses on user perception. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 401–415. IEEE (2019)

[31] Dencik, L., Leistert, O.: Critical perspectives on social media and protest: Between control and emancipation. Rowman & Littlefield (2015)

[32] Ems, L.: Twitter's place in the tussle: how old power struggles play out on a new stage. Media, Culture & Society 36(5), 720–731 (2014)

[33] Ermoshina, K., Halpin, H., Musiani, F.: Can Johnny build a protocol? co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols. In: European Workshop on Usable Security (2017)

[34] Fuchs, C.: Occupymedia!: The Occupy movement and social media in crisis capitalism. John Hunt Publishing (2014)

[35] Galletta, A.: Mastering the semi-structured interview and beyond: From research design to analysis and publication, vol. 18. NYU press (2013)

[36] Garms, L., Quaglia, E.A.: A new approach to modelling centralised reputation systems. In: Buchmann, J., Nitaj, A., eddine Rachidi, T. (eds.) AFRICACRYPT 19. LNCS, vol. 11627, pp. 429–447. Springer, Heidelberg (Jul 2019)

[37] Guberek, T., McDonald, A., Simioni, S., Mhaidli, A.H., Toyama, K., Schaub, F.: Keeping a low profile? Technology, risk and privacy among undocumented immigrants. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. pp. 1–15 (2018)

[38] Günther, C.G.: An identity-based key-exchange protocol. In: Quisquater, J.J., Vandewalle, J. (eds.) EUROCRYPT'89. LNCS, vol. 434, pp. 29–37. Springer, Heidelberg (Apr 1990)

[39] Gürses, S., Kundnani, A., Van Hoboken, J.: Crypto and empire: the contradictions of counter-surveillance advocacy. Media, Culture & Society 38(4), 576–590 (2016)

[40] Haciyakupoglu, G., Zhang, W.: Social media and trust during the Gezi protests in Turkey. Journal of computer-mediated communication 20(4), 450–466 (2015)

[41] Hale, E.: Hong Kong protesters use new flashmob strategy to avoid arrest. https://web.archive.org/web/20191101112411/https://www.theguardian.com/world/2019/oct/13/hong-kong-protesters-flashmobs-blossom-everywhere (Oct 2019)

[42] Halpin, H., Ermoshina, K., Musiani, F.: Co-ordinating developers and high-risk users of privacy-enhanced secure messaging protocols. In: Cremers, C., Lehmann, A. (eds.) Security Standardisation Research - 4th International Conference, SSR 2018. Lecture Notes in Computer Science, vol. 11322, pp. 56–75. Springer (2018), https://doi.org/10.1007/978-3-030-04762-7_4

[43] Hammersley, M., Atkinson, P.: Ethnography: Principles in Practice. Routledge (2007)

[44] Harlow, S.: Social media and social movements: Facebook and an online guatemalan justice movement that moved offline. New Media & Society 14(2), 225–243 (2012)

[45] Hennink, M.M., Kaiser, B.N., Marconi, V.C.: Code saturation versus meaning saturation: how many interviews are enough? Qualitative health research 27(4), 591–608 (2017)

[46] Herbert, S.: For ethnography. Progress in human geography 24(4), 550–568 (2000)

[47] Holbig, H.: Be water, my friend: Hong Kong's 2019 anti-extradition protests. International Journal of Sociology 50(4), 325–337 (2020)

[48] Howard, P.N., Hussain, M.M.: Democracy's fourth wave?: digital media and the Arab Spring. Oxford University Press (2013)

[49] Hui, M.: Hong Kong is exporting its protest techniques around the world. https://web.archive.org/web/20201009153848/https://qz.com/1728078/be-water-catalonia-protesters-learn-from-hong-kong/ (Oct 2019)

[50] 2015 IEEE Symposium on Security and Privacy. IEEE Computer Society Press (May 2015)

[51] International, Q.: Nvivo. https://web.archive.org/web/20200919072726/https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/about/nvivo (Sep 2020)

[52] Ion, I., Reeder, R., Consolvo, S.: "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 327–346 (2015)

[53] Jaggard, A.D., Syverson, P.: Onions in the crosshairs: When the man really is out to get you. In: Proceedings of the 2017 on Workshop on Privacy in the Electronic Society. pp. 141–151 (2017)

[54] Jakobsen, J., Orlandi, C.: On the CCA (in)security of MTProto. Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM'16 (2016), http://dx.doi.org/10.1145/2994459.2994468

[55] Jensen, R.B., Coles-Kemp, L., Talhouk, R.: When the civic turn turns digital: Designing safe and secure refugee resettlement. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–14 (2020)

[56] Johnston, A., Di Gangi, P., Howard, J., Worrell, J.L.: It takes a village: Understanding the collective security efficacy of employee groups. Journal of the Association for Information Systems 20(3), 3 (2019)

[57] Kamara, S.: Crypto for the People. https://www.youtube.com/watch?v=Ygq9ci0GFhA (Aug 2020), invited talk at CRYPTO 2020

[58] Kavada, A.: Creating the collective: social media, the Occupy movement and its constitution as a collective actor. Information, Communication & Society 18(8), 872–886 (2015)

[59] Kobeissi, N.: Formal Verification for Real-World Cryptographic Protocols and Implementations. Theses, INRIA Paris ; Ecole Normale Supérieure de Paris - ENS Paris (Dec 2018), https://hal.inria.fr/tel-01950884

[60] Koetsier, J.: Hong Kong protestors using mesh messaging app china can't block: Usage up 3685%. https://web.archive.org/web/20200411154603/https://www.forbes.com/sites/johnkoetsier/2019/09/02/hong-kong-protestors-using-mesh-messaging-app-china-cant-block-usage-up-3685/ (Sep 2019)

[61] Kow, Y.M., Nardi, B., Cheng, W.K.: Be water: Technologies in the leaderless anti-elab movement in hong kong. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2020)

[62] Krawczyk, H.: HMQV: A high-performance secure Diffie-Hellman protocol. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 546–566. Springer, Heidelberg (Aug 2005)

[63] Lab, T.C.: NSO Group / Q Cyber Technologies: Over one hundred new abuse cases. https://web.archive.org/web/20200419152528/https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/ (Oct 2019)

[64] Lee, F.: Solidarity in the Anti-Extradition Bill movement in Hong Kong. Critical Asian Studies pp. 1–15 (2020)

[65] Lee, F.L.: Internet, citizen self-mobilisation, and social movement organisations in environmental collective action campaigns: Two Hong Kong cases. Environmental Politics 24(2), 308–325 (2015)

[66] Lee, F.L., Chan, J.M.: Media, social mobilisation and mass protests in post-colonial Hong Kong: The power of a critical event. Routledge (2010)

[67] Lee, F.L., Chan, J.M.: Digital media activities and mode of participation in a protest campaign: A study of the Umbrella Movement. Information, Communication & Society 19(1), 4–22 (2016)

[68] Lee, F.L., Chan, M., Chen, H.T.: Social media and protest attitudes during movement abeyance: A study of Hong Kong university students. International Journal of Communication 14, 20 (2020)

[69] Lee, F.L., Yuen, S., Tang, G., Cheng, E.W.: Hong Kong's summer of uprising. China Review 19(4), 1–32 (2019)

[70] Lerner, A., He, H.Y., Kawakami, A., Zeamer, S.C., Hoyle, R.: Privacy and activism in the transgender community. In: ACM CHI. pp. 1–13 (2020)

[71] Lerner, A., Zeng, E., Roesner, F.: Confidante: Usable encrypted email: A case study with lawyers and journalists. In: 2017 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 385–400. IEEE (2017)

[72] Life360: Life360. https://web.archive.org/web/20200919000732/https://www.life360.com/intl/ (Sep 2020)

[73] Margetts, H., John, P., Hale, S., Yasseri, T.: Political turbulence: How social media shape collective action. Princeton University Press (2015)

[74] McGregor, S.E., Charters, P., Holliday, T., Roesner, F.: Investigating the computer security practices and needs of journalists. In: Jung, J., Holz, T. (eds.) USENIX Security 2015. pp. 399–414. USENIX Association (Aug 2015)

[75] McGregor, S.E., Roesner, F., Caine, K.: Individual versus organizational computer security and privacy concerns in journalism. Proceedings on Privacy Enhancing Technologies 2016(4), 418–435 (2016)

[76] McLaughlin, J.: Report: Arab Gulf states are surveiling, imprisoning, and silencing activists for social media posts. https://web.archive.org/web/20201015114424/https://theintercept.com/2016/11/01/report-arab-gulf-states-are-surveiling-imprisoning-and-silencing-activists-for-social-media-posts/ (Nov 2016)

[77] Mortensen, M., Neumayer, C., Poell, T.: Social media materialities and protest: Critical reflections. Routledge (2018)

[78] Mozur, P.: In Hong Kong protests, faces become weapons. https://web.archive.org/web/20190726093243/https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html (Jul 2019)

[79] Mukherjee, R.: Mobile witnessing on WhatsApp: Vigilante virality and the anatomy of mob lynching. South Asian Popular Culture pp. 1–23 (2020)

[80] Newman, L.H.: How cryptography lets down marginalized communities. https://web.archive.org/save/https://www.wired.com/story/seny-kamara-crypto-encryption-underserved-communities/ (Aug 2020)

[81] Nielsen, R.K.: Mundane internet tools, the risk of exclusion, and reflexive movements—Occupy Wall Street and political uses of digital networked technologies. The Sociological Quarterly 54(2), 173–177 (2013)

[82] Ohlheiser, A.: 'don't leave campus': Parents are now using tracking apps to watch their kids at college. https://web.archive.org/web/20200623143004/https://www.washingtonpost.com/technology/2019/10/22/dont-leave-campus-parents-are-now-using-tracking-apps-watch-their-kids-college/ (Oct 2019)

[83] Pavlov, E., Rosenschein, J.S., Topol, Z.: Supporting privacy in decentralized additive reputation systems. In: Jensen, C.D., Poslad, S., Dimitrakos, T. (eds.) Trust Management, Second International Conference, iTrust 2004, Oxford, UK, March 29 - April 1, 2004, Proceedings. Lecture Notes in Computer Science, vol. 2995, pp. 108–119. Springer (2004)

[84] Purohit, K.: WhatsApp to Bridgefy, what Hong Kong taught India's leaderless protesters. http://web.archive.org/web/20200406103939/https://www.scmp.com/week-asia/politics/article/3042633/whatsapp-bridgefy-what-hong-kong-taught-indias-leaderless (Dec 2019)

[85] Richards, T., Richards, L.: Using hierarchical categories in qualitative data analysis. Computer-aided qualitative data analysis: Theory, methods, and practice pp. 80–95 (1995)

[86] Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (Dec 2001)

[87] S. Ku, A.: New forms of youth activism – Hong Kong's Anti-Extradition Bill movement in the local-national-global nexus. Space and Polity 24(1), 111–117 (2020)

[88] Saldaña, J.: The coding manual for qualitative researchers. Sage (2015)

[89] Schröder, S., Huber, M., Wind, D., Rottermanner, C.: When SIGNAL hits the fan: On the usability and security of state-of-the-art secure mobile messaging. In: European Workshop on Usable Security. IEEE (2016)

[90] SCMP: Hong Kong national security law full text. https://web.archive.org/web/20201015085806/https://www.scmp.com/news/hong-kong/politics/article/3091595/hong-kong-national-security-law-read-full-text (Jul 2020)

[91] Scott-Railton, J.: Security for the high-risk user: separate and unequal. IEEE Security & Privacy 14(2), 79–87 (2016)

[92] Shirky, C.: The political power of social media: Technology, the public sphere, and political change. Foreign affairs pp. 28–41 (2011)

[93] Signal: Delete messages and alerts. http://web.archive.org/web/20210126184118/https://support.signal.org/hc/en-us/articles/360007320491-Delete-messages-and-alerts (Oct 2020)

[94] Simko, L., Lerner, A., Ibtasam, S., Roesner, F., Kohno, T.: Computer security and privacy for refugees in the united states. In: 2018 IEEE Symposium on Security and Privacy. pp. 409–423. IEEE Computer Society Press (May 2018)

[95] Skoric, M.M., Poor, N.D., Liao, Y., Tang, S.W.H.: Online organization of an offline protest: From social to traditional media and back. In: 2011 44th Hawaii International Conference on System Sciences. pp. 1–8. IEEE (2011)

[96] Sowers, J., Toensing, C.: The journey to Tahrir: revolution, protest, and social change in Egypt. Verso Books (2012)

[97] Sullivan, N., Turner, S., Kaduk, B., Cohn-Gordon, K., et al.: Messaging Layer Security (mls). https://datatracker.ietf.org/wg/mls/about/ (Nov 2018)

[98] Sušánka, T., Kokeš, J.: Security analysis of the Telegram IM. In: Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium. pp. 1–8 (2017)

[99] Tang, D.: Hong Kong protesters use 'chat groups' to organise rebellion. https://web.archive.org/web/20191219053015/https://www.thetimes.co.uk/article/protesters-use-chat-groups-to-organise-hong-kong-rebellion-xh3cq965h (Aug 2019)

[100] Telegram: Scheduled messages, reminders, custom cloud themes and more privacy. hhttp://web.archive.org/web/20200809190827/https://telegram.org/blog/scheduled-reminders-themes#new-privacy-settings (Sep 2019)

[101] Telegram: Search filters, anonymous admins, channel comments and more. http://web.archive.org/web/20201010041046/https://telegram.org/blog/filters-anonymous-admins-comments/#anonymous-group-admins (Sep 2020)

[102] Telegram: Bot api. https://core.telegram.org/bots (Jan 2021)

[103] The Stand News: In Hong Kong, authorities arrest the administrator of a Telegram protest group—and force him to hand over a list of its members. https://web.archive.org/save/https://globalvoices.org/2019/06/14/in-hong-kong-authorities-arrest-the-administrator-of-a-telegram-protest-group-and-force-him-to-hand-over-a-list-of-its-members/ (Jun 2019)

[104] Ting, T.y.: From 'be water'to 'be fire': nascent smart mob and networked protests in Hong Kong. Social Movement Studies 19(3), 362–368 (2020)

[105] Tremayne, M.: Anatomy of protest in the digital era: A network analysis of Twitter and Occupy Wall Street. Social Movement Studies 13(1), 110–126 (2014)

[106] Treré, E.: Reclaiming, proclaiming, and maintaining collective identity in the #yosoy132 movement in Mexico: an examination of digital frontstage and backstage activism through social media and instant messaging platforms. Information, Communication & Society 18(8), 901–915 (2015)

[107] Treré, E.: The banality of WhatsApp: On the everyday politics of backstage activism in Mexico and Spain. First Monday (2020)

[108] Tsui, L.: The coming colonization of Hong Kong cyberspace: government responses to the use of new technologies by the umbrella movement. Chinese Journal of Communication 8(4), 1–9 (2015)

[109] Tufekci, Z., Wilson, C.: Social media and the decision to participate in political protest: Observations from Tahrir Square. Journal of communication 62(2), 363–379 (2012)

[110] Uwalaka, T., Rickard, S., Watkins, J.: Mobile social networking applications and the 2012 Occupy Nigeria protest. Journal of African Media Studies 10(1), 3–19 (2018)

[111] Valeriani, A., Vaccari, C.: Political talk on mobile instant messaging services: a comparative analysis of Germany, Italy, and the UK. Information, Communication & Society 21(11), 1715–1731 (2018)

[112] Van Laer, J., Van Aelst, P.: Internet and social movement action repertoires: Opportunities and limitations. Information, Communication & Society 13(8), 1146–1171 (2010)

[113] Vaziripour, E., Wu, J., Farahbakhsh, R., Seamons, K., O'Neill, M., Zappala, D.: A survey of the privacy preferences and practices of Iranian users of Telegram. In: Workshop on Usable Security (USEC) (2018)

[114] Vaziripour, E., Wu, J., O'Neill, M., Metro, D., Cockrell, J., Moffett, T., Whitehead, J., Bonner, N., Seamons, K., Zappala, D.: Action needed! helping users find and complete the authentication ceremony in signal. In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). pp. 47–62 (2018)

[115] Vaziripour, E., Wu, J., O'Neill, M., Whitehead, J., Heidbrink, S., Seamons, K., Zappala, D.: Is that you, alice? a usability study of the authentication ceremony of secure messaging applications. In: Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017). pp. 29–47 (2017)

[116] Watson, H., Moju-Igbene, E., Kumari, A., Das, S.: "we hold each other accountable": Unpacking how social groups approach cybersecurity and privacy together. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. pp. 1–12 (2020)

[117] Wu, S.: Open homes, free rides: the people helping Hong Kong's protesters. https://web.archive.org/web/20210125144018/https://www.reuters.com/article/us-hongkong-protests-shelter-insight/open-homes-free-rides-the-people-helping-hong-kongs-protesters-idUSKBN1XU1G1?edition-redirect=ca (Nov 2019)

[118] Zhai, E., Wolinsky, D.I., Chen, R., Syta, E., Teng, C., Ford, B.: AnonRep: Towards tracking-resistant anonymous reputation. In: Argyraki, K.J., Isaacs, R. (eds.) 13th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2016, Santa Clara, CA, USA, March 16-18, 2016. pp. 583–596. USENIX Association (2016)

[119] Gil de Zúñiga, H., Ardèvol-Abreu, A., Casero-Ripollés, A.: WhatsApp political discussion, conventional participation and activism: exploring direct, indirect and generational effects. Information, Communication & Society pp. 1–18 (2019)